Public Comment Received Regarding Notice of Security Breaches

Comments listed in order received | Comments appear bolded | Editorial notes and changes appear [bracketed]

Comment number:	1	Commenter:	Mike Stollenwerk
Organization:	Fairfax County Privacy Council	Title:	Chairman

[Comments edited by JCOTS staff due to submission's length; every attempt has been made to include all specific comments regarding the draft legislation in question.]

[From page 5 of comments:]

Fairfax County Privacy Council supports these proposals but urges that Va. Code Section 59.1-444(A) be modified so to ensure that the $100 penalty does NOT require proof of "actual damages."

Comment number:	2	Commenter:	Greg Thomas
Organization:	Symantec Corporation	Title:	Manager, Eastern States Govt. Rel.

[Comments edited by JCOTS staff due to submission's length; every attempt has been made to include all specific comments regarding the draft legislation in question.]

[From page 1 of comments:]

Generally, Symantec is concerned with the vagueness of language regarding what constitutes a breach and what the disclosure has to include.

These provisions appear to be based on the definition of breach as requiring actual "unauthorized acquisition" of information that "compromises" security, confidentiality, or integrity. Symantec is concerned that this is overly broad language in the context of the definition and could arguably include not only a disclosure or acquisition of the actual personal information, but also disclosure or acquisition of any information that creates a risk of such disclosure or acquisition. In the absence of a narrower definition, one could assume a broad interpretation, including leaving a door unlocked, experiencing a physical break-in or losing a piece of paper with a password on it.

Symantec's interpretation of the legislation is that the notice requirement is only activated if someone acquires, or is reasonably believed to have acquired, personal information.

[From page 2 of comments:]

However, once activated, it is not exactly clear what "disclose any breach" means. For example, would a person or agency be required to just provide a simple notice that a "breach" has occurred, or does "disclose the breach" require a detailed description of the nature of the breach? Also, is the notice requirement limited to the people whose personal information is at issue, or is it necessary to broadly provide notice to all persons whose personal information is in the possession of the breached agency or person.

An assumed violation creates a private right of action, including the possibility of class action lawsuits, with damages of $100 per violation or actual damages.

[Virginia does not allow class actions.]

We would urge you to examine the California law when putting the finishing touches on the Commonwealth's legislation.

[This statute is the same language as the California law.]

Comment number:	3	Commenter:	Marc-Anthony Signorino
Organization:	AeA	Title:	Coord., State Leg. & Reg. Policy

[Comments edited by JCOTS staff due to submission's length; every attempt has been made to include all specific comments regarding the draft legislation in question.]

[From page 2 of comments:]

Mandating notice will lead to loss of consumer confidence in e-commerce and e-government. ... We strongly encourage the Joint Commission to reconsider the notice of breach requirement.

Critical definitions are vague, and could lead to significant confusion. ... If the definition of "breach of the security of the system" is to be taken at its most expansive meaning, it is seemingly in conflict with the proposed mandate made later in the bill (§ 59.1-443.3(B)). This mandate could be construed so that the notice requirement is only activated if someone acquires, or is reasonably believed to have acquired personal information.

[The bill requires notice only "following discovery or notification of the breach in the security of the data to any resident of the Commonwealth whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."]

However, once activated, it is not exactly clear what "disclose any breach" means. ... Second, it is unclear whether the notice requirement is limited to people whose personal information is at issue, or is it necessary to broadly provide notice to all persons whose personal information is in the possession of the breached agency or person.

[The bill only requires that person provide notice of the breach to "any resident of the Commonwealth whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."]

Lack of requirements regarding the consumer notice will lead to even more confusion - and possibly even litigation. ...

[The bill requires that the disclosure be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, ... or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.]

Immediate implementation of this legislation will expose businesses and the Commonwealth to unnecessary liability under the Act.

[All laws in Virginia become effective July 1 following enactment.]

Comment number:	4	Commenter:	J. Stephen Zielezienski
Organization:	American Insurance Association	Title:	Vice Pres. & Assoc. Gen. Counsel

[Comments edited by JCOTS staff due to submission's length; every attempt has been made to include all specific comments regarding the draft legislation in question.]

[From page 2 of comments:]

Proposed § 59.1-443.3 would generally require insurers to notify any Virginia resident whose nonpublic personal information had been accessed by an "unauthorized" person. AIA believes that insurers that comply with data security regulations issued by the Virginia Bureau of Insurance (or any other state insurance department) should be exempt from security breach notification legislation. The Gramm-Leach-Bliley Act of 1999 ("GLBA") requires regulators to adopt data security standards to be followed by insurers. The National Association of Insurance Commissioners ("NAIC") has developed a data security model regulation that has been adopted in the majority of U.S. insurance regulatory jurisdictions and provides for adequate data security protection.

[This bill deems these standards in compliance if "the person notifies subject persons in accordance with its policies in the event of a breach of security of the system" and allows these policies if the person ""maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part."]

Alternatively, as a jurisdiction like California that has adopted insurance privacy laws based on the 1982 NAIC model privacy law, Virginia should ensure that the security breach proposal follows California's breach of security law.

[This statute is the same language as the California law.]